

# PRIVACY DISTRIBUTED SYSTEM AND RECORDING MEDIUM

**Publication number:** JP2001034164 (A)

**Publication date:** 2001-02-09

**Inventor(s):** SAKURAI KOICHI; MIYAZAKI SHINGO +

**Applicant(s):** TOSHIBA CORP +

**Classification:**

- international: G06F12/14; G06F21/24; G09C1/00; H04L9/08; H04L9/10;  
G06F12/14; G06F21/00; G09C1/00; H04L9/08; H04L9/10;  
(IPC1-7): G06F12/14; G09C1/00; G09C1/00; H04L9/08;  
H04L9/10

- European: H04L9/08S

**Application number:** JP19990209891 19990723

**Priority number(s):** JP19990209891 19990723

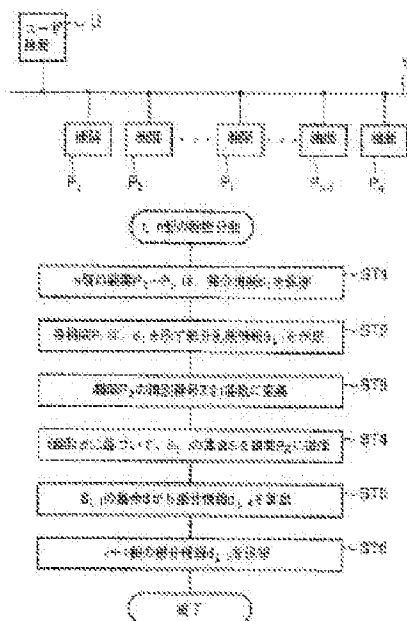
**Also published as:**

JP3560860 (B2)

US6810122 (B1)

**Abstract of JP 2001034164 (A)**

**PROBLEM TO BE SOLVED:** To realize a distributed decoding and signature by arbitrary (t) agencies among (n) agencies without calculating secret keys at environments where distributors are not present. **SOLUTION:** In this privacy distributed system, (n) respective agencies P1 to Pn preserve one of partial information di (0<=i<=n) of an (n, n) type and the partial information di are made to be t (r+1) of partial random numbers Sj of a (t, n) type and these (r+1) pieces of partial random numbers Sj are distributed to respective agencies P1 to Pn based on t-ary displays (tj-th value k, 0<=k<=t-1, 0<=i<=r) of identification numbers (z) of the respective agencies P1 to Pn and (r+1) of partial information dj, k are obtained by collecting partial random numbers distributed each other for every figure tj of the t-ary displays. Next, a user device U transmits ciphered data C by selecting (t) of agencies Tz and the (t) of agencies Tz answer partial outputs Xz which are obtained by them by arithmetically processing the ciphered data C based on the partial information di, k respectively to the user device U then, the device U composes the (t) of partial outputs Xz to obtain a decoded result.



Data supplied from the **espacenet** database — Worldwide